Amendments To The Claims

The listing of claims presented below will replace all prior versions, and listings, of claims in the application.

Listing of claims:

1. **(Currently Amended)** A method for realizing data security **storage and algorithm** storage by means of **a** semiconductor memory device, **wherein ~~comprising a semiconductor memory device,~~** the semiconductor memory device **~~comprising~~ comprises a** controller module as well as **a** universal interface module and **a** semiconductor storage medium module electrically connected with the controller module, respectively, characterized in that the method **~~of data security storage~~** comprises the steps of:

dividing the semiconductor storage medium module into at least two logic memory spaces;

using at least one of the logic memory spaces for storing **~~the~~** data to be protected;

setting up and storing a password**[[s]]** for the semiconductor memory device and said at least one logic memory space;

certifying the password before read/write operation;

when writing the data to be protected in the semiconductor memory device, the controller module receiving the data from the universal interface and, after **~~encryption~~ encrypting** the data, storing **[[it]]the encrypted data** in the semiconductor storage medium module; and

when reading the data to be protected from the semiconductor memory device, the controller module decrypting the data and transmitting the decrypted data via **[[a]]the** universal interface,

wherein at least one of the logic memory spaces is used for storing an algorithm, the controller module executes a designated algorithm according to input data from the universal interface and transmits a result of the execution via the universal interface.

2. (Canceled)

3. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of **a** semiconductor memory device of claim 1, characterized in that the semiconductor storage ~~**media**~~ **medium** module ~~**may be**~~ **comprises** a storage medium, or **a** combination**[[s]]** of at least two storage media.

4. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of **a** semiconductor memory device of claim 1, characterized in that the semiconductor memory device and**[[/or]]** said at least one logic memory space set up at least two levels of users passwords.

5. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of **a** semiconductor memory device of claim 4, characterized in that certification of user passwords ~~**may be**~~ **is** implemented before **[[the]]**operation in all logic memory spaces, ~~**and it may also be implemented**~~ **or** before **[[the]]**operation in the logic memory spaces storing the data to be protected.

6. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of **a** semiconductor memory device of claim 1, 4 or 5, characterized by setting up a database, and conducting **[[the]]**access and**[[/or]]** authority management to the data to be protected by way of the database.

7. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of **a** semiconductor memory device of claim 6, characterized in that the **authority** ~~**authorities**~~ comprise**s** reading **authority**, writing **authority**, modifying **authority**, deleting **authority** and executing ~~**authorities**~~ **authority**, each authority having the meaning of:

Reading authority: only allowing reading record data in the database;

Writing authority: only allowing writing new data in the database, but not covering

the record data with the same record title;

Modifying authority: only allowing writing data in the database and covering the record data with the same record title;

Deleting authority: allowing deleting the database or **[[the]]**records therein;

Executing authority: allowing executing record codes in the database, which is an authority with respect to ~~written data of~~ a self-defined algorithm or function code and it is ~~normally~~ invalid to designate an executing authority for normal record data.

8. **(Currently Amended)** The method for realizing data security **storage and algorithm** storage by means of a semiconductor memory device of claim 1, characterized in that at least one of the logic memory spaces is used for storing**[[the]]** data that does not need protection.

9. **(Currently Amended)** The method for realizing data security **storage and algorithm** storage by means of a semiconductor memory device of claim 1, characterized **in that an anti-falsifying identification is performed to** ~~by~~ identify**[[ing]]** whether the transmitted **[[and/]]**or stored data is falsified or not.

10. **(Currently Amended)** The method for realizing data security **storage and algorithm** storage by means of a semiconductor memory device of claim 9, characterized in that during transmitting or storing data, the ~~anti-falsification~~ **anti-falsifying** identification comprises the steps of:

A. invoking an encrypting algorithm to convert original data to obtain a conversion value X;

B. packing the original data and the conversion value X according to ~~certain~~ a format to form a data package;

C. transmitting or storing the ~~whole~~ data package; and

during receiving **[[and]]**or reading **[[the]]**data, the **anti-falsifying identification** ~~method~~ comprises the steps of:

A. unpacking the data package according to the ~~aforesaid same~~ format to obtain the **unpacked** original data and the conversion value X ~~of the original data~~;

B. invoking the encrypting algorithm ~~the same as the aforesaid one~~ to calculate a conversion value of the **unpacked** original data to obtain a conversion value Y;

C. comparing the calculated conversion value Y and the ~~received~~ conversion value X to see whether they are equal to each other;

D. if the compared result is **that Y and X are** equal, indicating the data that ~~have~~ **has** not been falsified, and otherwise indicating **that** the data ~~having~~ **has** been falsified.

11. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of a semiconductor memory device of claim 1 or 9, characterized by using randomly changeable session key to encrypt the data during the data transmission.

12. **(Currently Amended)** The method for realizing data security **storage and algorithm** storage by means of a semiconductor memory device of claim 11, characterized in that the step of using randomly changeable session key to encrypt data comprises the steps of:

A. at the beginning of the data transmission, transmission end transmitting a ~~command~~ **request** of exchanging session key and introducing at least one random number ~~at the same time~~;

B. after receiving the exchanging session key request, the semiconductor memory device randomly creating at least one random number, converting the received random number and the created random number by **[[the]]a key generating** algorithm to produce a session key, and then returning the random number created by the semiconductor memory device to the transmission end;

C. after the transmission end receives the returned random number, converting the ~~received~~ **returned** random number and the random number introduced by the transmission end itself with the ~~same~~ **key generating** algorithm to produce the session key.

13. (**Currently Amended**) The method for realizing data security **storage and algorithm** storage by means of a semiconductor memory device of claim 1,

characterized in that the data to be protected include[[,]] ~~but not limited to,~~ documents, passwords, cipher keys, account numbers, digital certificates, encrypting algorithm, self-~~defining~~ defined algorithm, user information and user self-defined data.

14. (**Currently Amended**) A method for realizing algorithm storage by means of a semiconductor memory device, ~~including~~ wherein [[a]]the semiconductor memory device ~~that~~ comprises a controller module, and a universal interface module and a semiconductor storage medium module that are electrically connected with the controller module, respectively, characterized in that the method ~~of algorithm storage~~ comprises the steps of:

dividing the semiconductor storage medium module into at least two logic memory spaces;

using at least one of the logic memory spaces for storing an algorithm;

the controller module receiving input data from the universal interface;

the controller module executing [[the]] a designated algorithm according to the input data, and transmitting a result of the ~~operation~~ execution ~~result~~ via the universal interface.

15. (**Currently Amended**) The method for realizing algorithm storage by means of a semiconductor memory device of claim 14, characterized in that the semiconductor storage medium module ~~may be~~ comprises a storage medium, or a combination of at least two storage media.

16. (**Currently Amended**) The method for realizing algorithm storage by means of a semiconductor memory device of claim 14, characterized in that the algorithm is an algorithm or several algorithms.

17. (**Currently Amended**) The method for realizing algorithm storage by means of a semiconductor memory device of claim 14, characterized in that the algorithm is an algorithm built in the semiconductor memory device or a self-defined algorithm or an encrypting algorithm.

18. (**Currently Amended**) The method for realizing algorithm storage by means of **a** semiconductor memory device of claim 14, characterized **[[by]]in that an anti-falsifying identification is performed to** identify**[[ing]]** whether the transmitted **[[and/]]**or stored data is falsified or not.

19. (**Currently Amended**) The method for realizing algorithm storage by means of **a** semiconductor memory device of claim 18, characterized in that ~~when~~ **during** transmitting or storing the data the anti-falsifying identification comprises the steps of:

A. invoking an encrypting algorithm to convert original data to obtain **a** conversion value X;

B. packing the original data and the conversion value X according to ~~certain~~ **a** format to form a data package;

C. transmitting or storing the ~~whole~~ data package; and

during receiving or reading data the ~~method~~ **anti-falsifying identification** comprises the steps of:

A. unpacking the data package according to the ~~aforesaid~~ format to obtain the unpacked original data and the conversion value X ~~of the original data~~;

B. invoking the encrypting algorithm ~~the same as the above one~~ to calculate **a** conversion value of the **unpacked** original **data** to obtain **a** conversion value Y;

C. comparing the calculated conversion value Y and the ~~received~~ conversion value X to see whether they are equal to each other

D. if the compared result is **that Y and X are** equal, indicating the data has not been falsified, and otherwise indicating that the data has been falsified.

20. (**Currently Amended**) The method for realizing algorithm storage by means of **a** semiconductor memory device of claim 14 or 18, characterized by using a randomly changeable session key to encrypt the data during the data transmission.

21. (**Currently Amended**) The method for realizing algorithm storage by means of **a** semiconductor memory device of claim 20, characterized in that the step of using

randomly changeable ~~talking cipher~~ **session** key to encrypt data comprises the steps of:

A. at the beginning of the data transmission, transmission end transmitting a ~~command~~ **request** of exchanging ~~talking cipher~~ **session** key and introducing at least one random number ~~at the same time~~;

B. after receiving the exchanging session key request, the semiconductor memory device creating randomly at least one random number, converting the received random number and the created random number by **[[the]]a key generating** algorithm to produce a session key, and then returning the random number created by the semiconductor memory device to the transmission end;

C. after the transmission end receives the returned random number, converting the **returned** ~~received~~ random number and the random number introduced by the transmission end itself with the **key generating** ~~same~~ algorithm to produce the session key.